REMARKS

Claims 1-3 are pending in the above-referenced application.

In the Office Action, Claims 1-3 have been rejected under 35 U.S.C. §102 (b) as being anticipated by "Intrusion Detection Using Static Analysis" to Wagner (hereinafter, "Wagner").

In making the rejection, the Examiner alleges that Wagner discloses a method for detecting malicious scripts using a static analysis comprising the step of checking whether a series of methods constructing a malicious code pattern exists and whether parameters and return values associated between the methods match each other as recited in Claim 1 of the present application. In support of the Examiner position the Examiner directs the Applicants attention to page 158, first paragraph of Wagner. However, for the reasons discussed below the Applicants respectfully disagree and traverse the rejection.

Upon closer review of Wagner in general and the section cited by the Examiner in particular, Wagner clearly indicates that the disclosed method of Wagner actually *"prunes away all other aspects of the model, even to the point of disregarding the contents of local variables, data structures, and all other data flow."* In fact, one problem that Wagner discusses is that transition systems derived from the source are usually too complex to be useful. (See page 157, last paragraph). Wagner also states that one way to "tackle these problems is by simplifying the transition system greatly, abstracting away unnecessary complexity." (See page 158, Col. 1, lines 1-2). In fact, Wagner unambiguously

states that *"since we only care about the sequence of system calls issued, we prune away all other aspects if the model, even to the point of disregarding the contents of local variables, data structures and all other data flow."* (See page 158, Col. 1, lines 3-6).

In stark contrast, Claims 1-3 of the present invention checks not only the *"series of methods conducting a malicious code pattern"*, but also *"return values associated between the methods."* In addition, the method of the present invention generates instances of the matching rule by searching for *code patterns* matched with the matching rule from a relevant script code to be detected. (See Claim 1). However, the matching step of the present invention is neither taught or suggested by Wagner since Wagner specifically teaches that *"all other data flow is stripped from the model first"* making matching rule step of the present invention impossible. In other words, since Wagner teaches to strip all other data flow from the model first, data is not even available in Wagner method that can be used in the matching step of the present invention.

Since each and every element must be present in a single reference in order to anticipate a claim, and as discussed above, Wagner fails to teach or suggest generating instances of the matching rule by searching for code patterns matched with the matching rule from a relevant script code to be detected, the rejection of Claims 1-3 under 35 U.S.C.§102 (b) over Wagner must be reconsidered and withdrawn.

Moreover, since Wagner teaches to *"prune away all other data flow"* first, making it impossible to carry out this required step, Wagner in essence teaches away from the present invention. For this further reason the

rejection of Claims 1-3 under 35 U.S.C.§102 (b) over Wagner must be reconsidered and withdrawn.

Since Claims 2 and 3 depend from Claim 1, they contain all of the limitations, attributes and features of Claim 1 and for the reasons discussed above it is respectfully requested that the rejection of Claims 2-3 under 35 U.S.C.§102(b) under Wagner be reconsidered and withdrawn.

In view of the foregoing, it is respectfully requested Claims 1-3 are in condition for allowance and the same is respectfully requested.

Respectfully submitted,

Leo G. Lenna
Attorney for Applicants

DILWORTH & BARRESE, LLP
333 Earle Ovington Blvd.
Uniondale, New York 11553
Phone: (516) 228-8484
Facsimile: (516) 228-8516